

5239
63D
12 Jun 00

From: Commander, Naval Supply Systems Command

Subj: INFORMATION ASSURANCE (IA) PROGRAM FOR THE NAVAL SUPPLY
SYSTEMS COMMAND

Ref: (a) OPNAVINST 5239.1B of 9 Nov 99
(b) DODINST 5200.40 of 30 Dec 97
(c) CNO Washington DC 152300Z Nov 99
(d) NAVSUPINST 5239.1A of 3 May 93

1. The security challenges confronting NAVSUP's information and information systems are multiplying rapidly with the exponential growth of interconnected systems for producing and exchanging data. As interconnectivity increases and the threats to information and information systems become more sophisticated and diverse, NAVSUP systems become inherently more vulnerable to surreptitious access and malicious attacks.

2. In light of the above factors, both our information and information systems must be properly developed, managed, and protected as required by law, regulation, or treaty. Facilitating the management and protection of our systems requires an appropriate commitment of personnel and other resources to implement security measures and to promote user awareness.

3. In support of the above goals, addressees will:

a. Execute the provisions of reference (a). As this comprehensive directive precludes the need for NAVSUP to maintain its own IA policy document, reference (d) is hereby cancelled. The NAVSUP Command IA Program Office will continue to centrally fund corporate initiatives, support local programs to the maximum practical extent, and disseminate specific implementation guidance as required.

b. Ensure the IA Program is adequately staffed. In view of the importance and growing responsibilities of this inherently-governmental function, this should be a full-time responsibility of at least one permanent government employee. If an activity

Subj: INFORMATION ASSURANCE (IA) PROGRAM FOR THE NAVAL SUPPLY
SYSTEMS COMMAND

is larger than 500 employees, a second or third individual
should be designated as staff to the Manager.

c. Promote and endorse an IA Awareness Program. This
program shall educate managers, developers, and users on current
IA initiatives. These initiatives should include, but not be
limited to, firewall policy, system certification and
accreditation requirements (reference b), Navy/Marine Corps
Intranet impact, redelegation of Designated Approval Authority
policy, on-line survey requirements, Information Condition
status, safe IA practices, and the corporate security program
strategy. Email, flyers, posters and videos are some of the
methods that can be used in implementing this program.

d. Ensure all systems administrators are Navy-IA System
certified as outlined in reference (c).

4. Our point of contact is Ms. Charlene F. Tallman, SUP 63D, at
717-605-1432 or DSN 430-1432.

/s/ Larry M. Glasco
Executive Director

DISTRIBUTUION:
(see page 3)

Subj: INFORMATION ASSURANCE (IA) PROGRAM FOR THE NAVAL SUPPLY
SYSTEMS

DISTRIBUTION:

FISC Jacksonville (Code CO)
FISC Norfolk (Code 00)
FISC Pearl Harbor (Code 00)
FISC Puget Sound (Code 00)
FISC San Diego (Code 00)
FISC Yokosuka (Code 00)
FMSO (Code 9)
FOSSAC (Code 00)
NALC Mechanicsburg (00)
NAVICP (Code 00)
NAVPETOFF (Code 00)
NAVTRANS (Code 00)
NEXCOM (Code 00)

Copy to:

FISC Jacksonville (Codes 30, DMX)
FISC Norfolk (Codes 82, 80.1)
FISC Pearl Harbor (Codes 95C/D, 09)
FISC Puget Sound (Code 43.3, 44)
FISC San Diego (Codes 032, 31)
FISC Yokosuka (Codes 31, 30IS)
FMSO (Codes 94, 941, 941-INFOSEC Team, 94E, 95B, 961)
FOSSAC (Code 01C)
NALC Indian Head (Code 091B)
NAVICP (Codes 041, 04E, 0416, 054, 0542, 05422.03, 0543, 05733,
M043, M0433.01, P045.25, P089, P0892, M0426, P042)
NAVPETOFF (Code 10)
NAVSUP (X32 and Codes 02XB, 33C)
NAVTRANS (Code 06)
NEXCOM (Code IA)